Smart Grid Support Network

J. Guasch Albareda
Masters in Smart Grids: Final Project
Scottish Power Energy Network
Glasgow, Scotland

Abstract— **The architecture of the firewalls in any critical infrastructure, such as the electrical grid, is the key to provide the security and reliability to those systems. This project worked with the different technologies and configurations available to update the current architecture of firewalls from Scottish Power. A unite and symmetric architecture, composed with pairs of high availability new generation firewalls from Palo Alto in active-active configuration was the final model proposed, due to the improvement in its performance results compared to the ones obtained in the current architecture.**

Index Terms—**firewalls, active/active, active/passive, availability.**

I. Introduction

Nowadays, in the context of a technology driven and interconnected world, the key to protect critical infrastructures, such as the electrical grid, is to design them to being able to be efficient and possess a secure management. The Smart Grids, which mixes information and communication technologies with the traditional electrical power systems, are changing the traditional perception of generating, distributing and consuming electricity. Nonetheless, with its increasing dependency in digital technologies, the possibility to suffer from cyber-attacks, being potential riskers to the security and reliability of those systems, has also increased.

A critical aspect to ensure the successful operation and implementation of Smart Grids is to integrate robust cybersecurity measures in its system. An essential asset for any secure information system is the firewall. They are fundamental components which take a key role in filtering and securing the communication in the Smart Grids' telecommunications network. Those barriers or gateways are the first line of defence, preventing malicious activity and undesired or unauthorised access.

The main focus of this project is to investigate and address the importance of a correct design in the firewall's architecture of the Scottish Power network. To do that a deep analysis on the different technologies, techniques and configurations will be carried.

In this paper, Section II will present the definition of the project, including context and reasoning behind the project. The section will also include the specific objectives to perform, and the methodology used for the achievement of the project. Section III will briefly present the characteristics of the current architecture of the firewalls, studying the different assets and characteristics in a high-level analysis. In the case of Section IV, a review on the operation of the Cisco FirePower firewalls will be performed, and in Section V, all firewalls technologies will be analysed to study which would be the best option for the final architecture. Furthermore, a review of the current routing techniques used will be covered in Section VI. Section VII will study the performance of both type of systems, active-active and active-passive systems. Also, Section VIII will propose a new architecture of firewalls and will compare its performance with the one currently used. Finally, Section X will present the conclusions of the paper and future related works.

II. Definition of the project

The Smart Grid Operations LAN consist of the RTS and Telecoms network devices segregated by the policy from respective Firewalls. These domains are managed separately, however both domains can overlap in the LAN to communicate with specific end point devices.

The current separation of RTS and Telecoms LAN domains is a consequence of the evolution of SPEN as a business and has resulted in a complexity which is impacting network performance.

Each domain uses their own Switches and Firewalls that are used to perform traffic filtering, route filtering and NAT (network address translation) which aid in keeping the domains separate but is now limiting options for system integration.

Scottish Power Energy Networks has started a programme to review and upgrade the IP Networking Infrastructure that underpins key elements of the SPEN Telecoms and RTS environments. The Smart Grid Support Network is defined as the functional working of servers and interconnecting infrastructure for the Network management platforms that support RTS and Telecoms networks. The objectives of this project are the following:

- Assessment of feasibility in consolidation of current Infrastructure Firewall Estate.
- Propose design of security focused firewall architecture, aligning with the Purdue Network Model.

- Assessment of available technologies to facilitate secure firewall architecture, including configuration management.
- Comparison of Active/Active and Active/Passive deployments.
- Assessment of networking technologies to optimize current routing landscape.

The methodology followed to achieve the different objectives of the project started with an extensive analysis of the current firewall's infrastructure. The different issues of the present architecture will be identified and recommendations to have an update in the actual performance will be presented.

These recommendations will then be considered in the proposition on a new design of the firewall's architecture, which main goal is focusing on security and redundancy while aligning with the Purdue Network Model. This new design will consider configuration management, routing techniques and the different High Availability to create a resilient and feasible model.

To achieve the final goal of the project, the use of different reports and information regarding the technologies and the techniques used will be reviewed and analysed. Moreover, different models of Simulink will be designed to, first, understand the behaviour of the current architecture, to finally create and correctly argue the new architecture's proposal.

III. Architecture's current state

As it was said in last section, currently RTS and Telecoms network devices work independently, each of the domains are managed separately. Even while being able to overlap themselves in the LAN to communicate with specific end point users, their firewalls are managed and designed completely different. This independency has caused at the end some inefficiencies in the performance of the network.

The system of study is conformed by 4 main networks. Those networks can be also divided in two sectors, the North Network is composed by the Kirkintilloch and Scottish Power House networks, while the South Network is composed by the Prenton and Wrexham network.

Apart from the differentiation between zones, the devices, specifically the firewalls used in the RTS, and Telecommunication network are completely different, even if their main goal is the same, filtering packets. The firewalls used in the Telecommunications network are the Cisco FirePower 2130 firewalls, those firewalls are configurated in a way that they create single points of failure, since if they fail the information cannot go through any other path.

On the other hand, the RTS network is designed we pair of high availability Palo Alto new-generation firewalls (NGFWs), which, at the moment, work in an active-passive configuration. This means that there is one firewall, the primary, which is constantly working until it fails. In the case of a failure, the backup firewall would start filtering, making possible to keep the filtering process and not stopping the flow of information.

Another aspect to take into consideration is how the system, comparing north and south, is not symmetric, which at the end makes it more difficult to operate, update or scale. In Figure 1, a high-level representation of the system which will be studies in this project is presented.

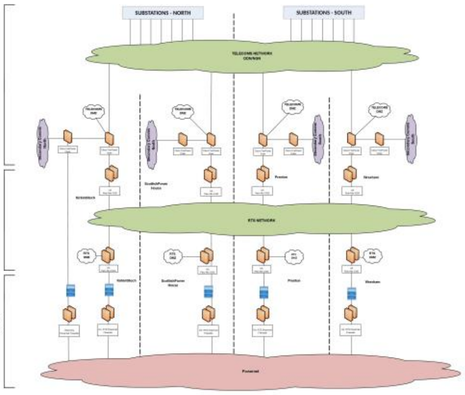


Figure 1: Architecture's current state

The new architecture will be intended to be designed in a way that the system achieves high redundancy with a high availability system. The final design must be capable to keep the information flowing, even in the case of a failure. In the following sections, a study of the actual and other firewalls technologies will be performed, considering its high availability configuration.

IV. Cisco's Firewalls Review

This section will analyze the part of the current architecture composed of Cisco's firewalls in order to finds the different issues of their operation. Also, it will include some recommendations for future updates.

The actual architecture of the firewalls inside the Telecommunications network is built with Cisco FirePower firewalls, from Cisco Advanced Services. A gap analysis was performed in order to provide a wide view of the current configuration, feature or functionality for Cisco FirePower in SPEN's network. The review of the architecture will study the following devices:

- Cisco FirePower Management Center (FMC) for VMWare v6.6.4 (x1).
- Cisco FirePower Management Center (FMC) for VMWare v6.6.a (x3).
- Cisco FirePower 2130 FTD v6.6.4 (x2).
- Cisco FirePower 2130 FTD v6.6.1 (x6).

A. General Architecture

Regarding Firewall Threat Detection (FTD), the configuration is not High Availability (HA). A HA or failover setup joins two devices so that if the considered as primary have any kind of failure or error, the other one, the secondary, takes over. With that configuration the network can keep operating while the failure is being analysed and treated. The recommendation for this case is to configurate the architecture with two, identically configurated, FTDs connected through a failover or state link. These devices will have to communicate over that link to determine which unit would operate the network and to synchronize any changes in their configuration if the failover link is the one adopted. For the case of state link, the system would pass information to a standby device to maintain the connection inn the network in the case of a failover event.

Analysing the operation of the Firewall Management Center (FMC) it was also studied the benefits that its configuration in HA would benefit the architecture. HA feature allows the user to manage devices with a redundant FMC, which would ensure the continuity of the operations. FMC can work under Active/Standby HA configuration, being the active the one unit which would manage the devices, and the standby unit the one which would not actively manage them. Synchronization to share communication within the units is essential, this feature would permit the active unit to write configuration data into a data store, replicating data in both units. It should be noted that, as in the FTD case, if the active FMC fails, the one in standby mode would take over and continue the operation in the network, promoting it as the new active unit.

B. Scottish Power House network

Focusing on Scottish Power House (SPH), three aspects have been studied: the Firewall Management Center (FMC) and the inner and outer firewall of its infrastructure. Regarding FMC several issues were analysed:

- Reporting missing: recommended to generate reports monthly for a better understanding of the operation of the unit.
- VDB automatic updates are missing: recommended to be daily checked to have an updated database, essential for the security from different vulnerabilities.
- Configure SNMP traps: no trap configured for the Access Control Policies, is a good practice to enable traps in the devices. It would save network resources and negatively impacting agent performances.
- Configure Change Reconciliation: recommended feature which is not currently implemented in the FMC configuration.

As regard to the firewalls other issues have been detected in the operation and configuration of these devices:

- CSS Styles loading issue in Chrome 85, IE and Edge browsers: the bug happening is the CSCvv5746 and is present on the latest version of Edge and Chrome browsers. This error occurs when the CSS is not getting applied when switching to a different theme. If the theme is not the default one and the browser is not the latest version, the issue appears. The recommendation of this issue is to set the device in unstable state when it occurs. Also, open the FDM UI in Firefox browser and switch to "Default Color Theme".
- Threat score disposition override setting decreased below default: the setting of the "Override AMP Cloud Disposition Based upon Threat Score" is established below 76 (Very High). To increase the security of the firewalls' operations, the value 76 is the setting recommended.
- Static route where the next-hop IP address is not the same IP subnet as the interface associated with the route: this feature can be critical since its used to determine the best path to efficiently send information and data to their final destination.

C. Kirkintilloch network

The Kirkintilloch network has also been deeply analyzed. The study, as in the case of SPH network, is divided in two technologies: FMC and firewalls. In the case of the Firewall Management Center, the founded issues had the same nature as the ones studied in SPH network. There are reporting and VDB automatic updates missing. Also, there are not traps configurated for Access Control Policies and no configuration for the change reconciliation.

Regarding firewalls, there's also loading problems from CSS Styles in browsers such as Chrome 85 or Edge and the threat score disposition setting is below the default one. In regard to firewalls there have been found new issues in the devices from this zone. There was a software crash detected in the last 30 days of the study because of a line crash and there was also a full usage of one of the firewalls, a review on the disk usage and the platform logs is recommended.

D. Prenton network

The Prenton network was also studied in the same way as the other environments. In the case of the Firewall Management Center, it was discovered that it had the same issues as the other zones, KRK and SPH. Reporting and VDB automatic updates missing and no configuration for SNMP traps. Focusing on firewalls, as it happened with the FMC, some issues of the same nature were found: CSS Style loading issue and threat score disposition override setting below the default configuration. A new and important problem found for one of this network's firewall is that the packet captures are configurated. This can potentially decrease performance and raise CPU from the device. Captures cause a CPU spike, this configuration should be used for troubleshooting traffic flow issues, and, after troubleshooting, the setting should be off.

E. Wrexham network

The analysis of Wrexham environment shown similar results, compared to the other networks already commented. Considering its FMC, reporting and VDB automatic updates are missing, and traps should be configurated for the Access Control Policy. For this specific environment only CSS Styles loading issues in browsers were contemplated in both firewalls.

V. ARCHITECTURE'S FIREWALLS REVIEW

This section will consist of a more technical review of, not only the firewalls that are being currently used, but also about the new model that is being considered for the future design of the infrastructure. After the study, a comparison between the different models will be performed.

A. *Cisco FirePower 2130*

The Cisco Firepower 2100 Series is a four-threat-focused security platform family which have the ability to deliver a higher performance threat defense and resiliency to the business and telecommunications infrastructure. Exceptional sustained performance can be achieved while their advanced threat functions are being used. Cisco Firepower 2100 Series' platforms incorporate a dual multicore CPU architecture which provides the system with firewall, threat inspection and detection, and cryptographic functionalities. Network Equipment Building Standards (NEBS)-compliance is supported by the model used in the TELECOM SYSTEM, the Cisco Firepower 2130 platform. These devices can operate with the Secure Firewall ASA or Threat Defense software [1].

B. *Palo Alto PA-3220 FW*

Palo Alto Networks PA-3200 Series appliances secure traffic, including the encrypted traffic with the use of processing and memory for security, management, networking, and threat prevention. PAN-OS software is the controlling element of these devices. The software can classify all traffic, which includes threats, contents and other applications, in order to traffic it to the user at any location and device type. The application, content and user will then be used to create the security policies, which will reduce incident response time and improve the security posture of the system. The key characteristics of these devices can be classified in different features: ML Powered, full Layer 7 inspection, security regardless of device or location, encrypted detection, centralized management and use of AIOps and cloud services among others [2].

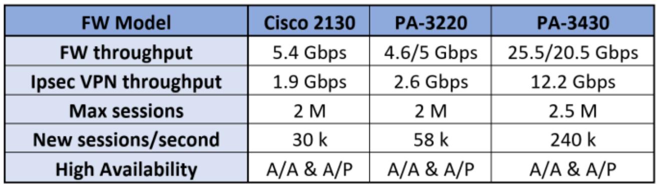
C. *Palo Alto PA-3430 FW*

This new model has most of the capabilities and features that the past PA firewalls had. PAN-OS software is still the one used to classify traffic, threats, and any content regardless of the device or the location. PA-3400 Series includes the key security and connectivity features that the PA-3200 Series had. The new series are still a machine learning powered firewall, with the capacity to learn from error threats to automatically detect new ones. They also have the ability to identify and categorize, with full layer 7 inspection, any port or application at any time. The series adapt policy based on user activity while enforcing security for the user, regardless of device and location. PA-3400 series can also detect malicious activity inside encrypted traffic and offer centralized management and visibility. They also prevent business disruption with AIOps, and its cloud-delivered security devices can detect and prevent unknown threats. As the PA-3200, the new series enables SD-WAN functionality and provides the user with a single-pass architecture service for packet processing. The main feature that these new series bring is the native web proxy support. They can unite firewall and proxy in one platform while still being able to manage capabilities through the centralized management software [3].

D. *Firewalls comparison*

The firewalls described above are the ones considered for the new architecture of the RTS and Telecommunication's network. Table 1 presents the most important capabilities and capacities which all the firewalls, already described, have.

Table 1: FW capabilities comparison



FW Model	Cisco 2130	PA-3220	PA-3430
FW throughput	5.4 Gbps	4.6/5 Gbps	25.5/20.5 Gbps
Ipsec VPN throughput	1.9 Gbps	2.6 Gbps	12.2 Gbps
Max sessions	2 M	2 M	2.5 M
New sessions/second	30 k	58 k	240 k
High Availability	A/A & A/P	A/A & A/P	A/A & A/P

The firewall throughput is the volume of traffic, in Gbps, that can pass through the firewall at any given time, this feature is a must since the network needs to have enough capacity to transport all the packets to have a complete view of the network. It can be seen how Cisco FirePower and PA-3220 firewalls have a similar capacity in terms of their throughput, but the PA-3430, as a new model have a capacity nearly 5 fives higher than the other models.

The IPsec VPN throughput is the measure that provides the amount of data that can be transported with IPsec VPN connection. High volume of data traffic needs to be possible to have remote accessible system which is reliable to the user. In the case of Cisco FirePower's firewalls, they are the models with the lower rate, which make them an unattractive option for future investments if remote control is a main part of the network operations.

The max sessions, as its name imply, are the maximum number of firewall sessions the device can support. On the other hand, the new sessions or connections per second are related to the pace in which the firewall can create and store new sessions. The total number of sessions that the different devices can manage are similar, with the PA-3430 model having the most, 2.5 million. The most distinctive feature is the new sessions per second, being the Palo Alto firewalls the one with better results. A network that is intended to transport, not only great amount of data, but also different data constantly, the new sessions per second feature is one that needs to be seriously considered.

In the case of their high availability configurations, all the models can work on active/active and active/passive configuration. This make it possible for the future architecture to have a flexible design, which could change in the future if there is any change regarding amount or typology of data and the size of the network.

VI. CURRENT ROUTING REVIEW

This section will perform a high-level analysis on the routing landscape of the networks composing the architecture. It is also dedicated to summarizing and describe some routing and administration practices that would help in the implementation of future implementations for new network designs. Firstly, it needs to be acknowledged that having a new routing design is a large fix and will need of a great amount of time and resources.

RTS and Telecoms networks are currently being managed and maintained by three different companies: Systal, Leidos and Magdalene. In the Telecoms network the firewalls are being managed by Leidos, but they will be changed by Systal in the future. This change will help with a quicker response in business-as-usual activities and any resolution regarding incidents, such as faults or malfunctions from assets managed by Systal.

As it was detailed during this section, there are two parts in the SPEN estate that differ not only in geographical terms, but also in some practices inside their networks. The North is characterized by the use of static routing to send traffic between devices or for default routes. On the other hand, the South networks use more dynamic routing protocols. This redundant method permits the change in the routing layout due to any failures of link or devices that might occur in the network, which make it a more advantageous option.

Another potential issue is the fact that in Telecoms network Cisco 2130 firewalls' setup is in such a way that creates a SPF, whereas in RTS network the Palo Alto FW are configurated as HA pairs, being more resilient to failures and permitting a more redundant architecture. For future network designs upgrades in the network regarding redundancy must be treated.

Finally, some OSPF practices that will need to be considered for future deployments or configuration of network are the following:

- Summarization Techniques: the summarization is essential for two main reasons, firstly, to limit the number of routes in an area, especially in the backbone. Secondly, it's important to minimise the impact of flapping links. These techniques can be really useful more intra-area routes. Also, in an area with multiple Area Border Routers (ABRs), which is also useful in terms of redundancy, summarization should be configurated in all ABRs. Even though it helps with redundancy, the number of ABRs needs to be reasonable, to limit the number of summary Link State Advertisements (LSAs) inside the domain.
- Router ID: use router-id command to configure a deterministic router ID for OSPF process. Choosing the router ID from the same OSPF area address space the router belongs to will be helpful for summarization for the cases in which the router IDs need to be routed.
- Process ID: it has local significance to the router, recommended to have the same for any router that works under the same OSPF domain. By making this, configuration consistency will be improved.
- Authentication: MD5 authentication between OSPF neighbors can be configured if security is a key feature of the network.
- Area Size: the routing table should not be big, not only in terms of possible routes, also routers.
- OSPF flood reduction: can be enabled on a router if it can be supported. This ability can minimize the LS aging process in a link device. This ability needs to be furtherly considered if neighboring router does not support DC bit mainly because it could be the case that it does not work.

VII. Active-active vs active-passive

The analysis in the configurations available in the firewalls from Palo Alto was carried to study which will have better results in terms of efficiency and performance. The analysis was made by designing and creating a Simulink model in MATLAB R2022b with the use of the SimEvents library [4].

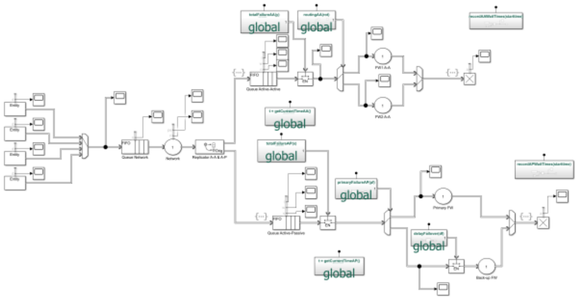


Figure 2: Simulink HA FW model

The model, shown in Figure 2, is composed by two different pairs of firewalls, one active-active and the other active-passive, in parallel that will receive packets overtime and have a probability to fail. In the case of the active-active configuration the packets will go through both firewalls, alternating from one another, if one of the firewalls fails the other one will continue filtering the packets by itself until it is repaired and operational. On the other hand, in the active-passive configuration, there will be one primary firewall which will process all the packets until a failure event occurs. In that case, the primary firewall will be disconnected and the other one, the back-up firewall, will start processing the packets until it is repaired.

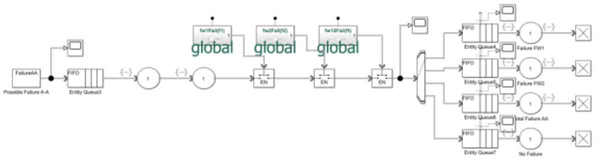


Figure 3: Active-active failure design

The failure of the firewalls is simulated with one model for active-active configuration and active-passive configuration, as shown in Figure 3 and Figure 4 respectively.

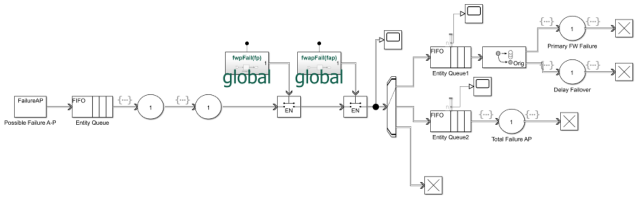


Figure 4: Active-passive failure diagram

That failure depends on a probability, which, in reality, is high. Different distributions were studied to see which was closer to the way in which the firewalls fail and to supervise the performance results that the different configurations obtained, those distributions were the following:

- Random distribution: there is a 5% of probability of failure. The model will generate random number between 0 and 1 for each firewall, if any of those numbers have a value below 0.05, a failure is detected, and the firewall is disconnected.

- Lognormal distribution: there is a 95% of probability that the firewall does not experience any failure. The model will generate a random number between 0 and 100, following the distribution with a mean of 5 and sigma of 0.5 and 1, if any of those numbers have a value above 95, a failure is detected, and the firewall is disconnected.

- Extreme value distribution: there is a 5% of probability of failure. The model will generate a random number between 0 and 100, following the distribution with a mean of 95 and sigma of 3 and 8, if any of those numbers have a value below 5, a failure is detected, and the firewall is disconnected.

The different distributions created different scenarios in the simulations of the performance of the configurations. At the end, the one used for the final architecture is the Extreme value distribution, since is the one closer to reality, experiencing no failures during the simulation. Regarding the performance of the different configurations, in all distributions the active-active options showed better results in terms of total throughput of packets and its total time waited to completely filtered and transmitted, being the reason why the configuration in chosen for the final architecture. Table 2 presents this behaviour, showing the comparison between active-active and active-passive results in a simulation of 10.000 seconds using the lognormal distribution as an example.

Table 2: Active-active vs active-passive, Lognormal Distribution (sigma 0.5)

Configuration	Active-Active	Active-Passive
Total throughput (packets)	6.532 e3	5.673 e3
Wait time peak (seconds)	368	917

VIII. Proposed architecture

This section will analyse the changes recommended for the new architecture of firewalls of all Scottish Power's networks. Some of the most applicable technologies have been already studied in last sections.

Cisco FirePower NGFWs in the Telecommunications networks originated a vast list of problems, being the single point of failure (SPF) the critical of all. This problem created scenarios in which, in case of a failure of one of those firewalls, the network was uncapable of transmitting information. Furthermore, it also was commented, how a transition to Palo Alto NGFWs would be the most reliable option at the moment, not only for their better capabilities, but also that, since all Palo Alto firewalls from the system can be managed and supervised through the Panorama software, their integration would reduce the complexity of operating them.

Moreover, it was also studied how, in a scenario were all firewalls used were from Palo Alto, the network will have high availability capabilities, uniting both, RTS and Telecommunications network. The two configurations available for this technology were active-active and active-passive, and both configurations would be beneficial and possible to implement in the new architecture. Since both had advantages and difficulties in its operation, last Capítulo helped to decide which would be optimal at the end. With the help of the different models and simulations used, implementing a pair of Palo Alto NGFWs in active-active configuration would have better results in term of performance, even if it also increases the complexity of the operation of those assets.

Finally, having updated the different networks, changing all firewalls or pair of firewalls, to an active-active pair of Palo Alto firewalls, another aspect commented in the beginning is also addressed for the final proposal. A symmetric system, between north and south, was also considered. That makes the hole system of networks look similar, reducing complications during the management of the different firewalls and the operation of transmitting information overall.

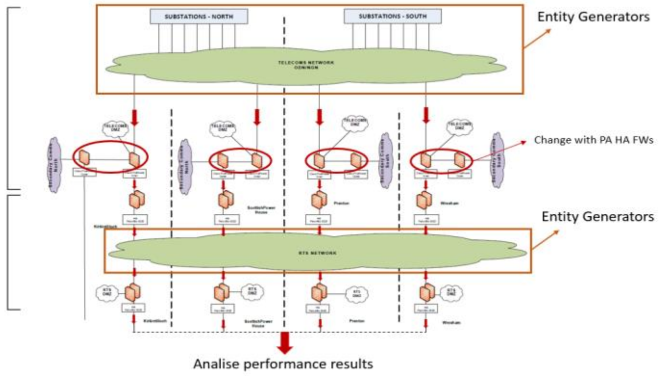


Figure 5: Proposed architecture

With that being said, Figure 5 shows the changes proposed for the new architecture of firewalls. The next subsection from this part of the project will analyse through other Simulink models the performance of the new architecture, compared to the current one which possesses SPFs.

Firstly, a definition of some technical specifications used for the design of the model will be presented with the presentation of the model itself. Then the next subsection will analyse both results, considering normal conditions, in which a failure of a firewall is nearly impossible using the Extreme Value Distribution used in last section. Finally, the last one will increase the probability of failure, using the constant scenario from last section, to see how the two systems behave and perform during failure scenarios.

A. *Technical specifications and model*

This part of the paper will cover the different technical specifications considered during the design of the Simulink's model traying to recreate both, the current and the proposed architecture.

The model is divided in two parts, the recreation of every network, and the model simulating the possible failure of every firewall of those networks. The networks are divided in two different areas:

- North Network: this area is composed by the Kirkintilloch network and the Scottish Power House network.
- South Network: this area is composed by the Prenton network and the Wrexham network.

As it was presented before, symmetry is one of the focuses, so networks are the same, in terms of features, technologies and behaviour. This condition will create scenarios in which all networks share similar performance results. All those networks have a similar architecture as the model used for the active-active vs. active-passive models. The main differences are, as seen in Figure 5, there will be 3 clusters of firewalls and two parts where entities are generated, the ones coming from the telecommunication network and the ones coming from the RTS network. The entity generators will follow the same behaviour as the ones used in the simulations from last section, both are composed by group of four generators, generating packets with a size of 4 Mbps with an intergeneration time action following Equation 1, being rand(1,1) a function which generates a random number between 0 and 1:

Equation 1: Entity generator intergeneration time action

$$dt = 1 \cdot \log\left(1 - rand(1,1)\right)$$

In the same way as in the simulations from last section, network itself is considered, using cat6 with a capacity that goes between 100 Mbps and 1 Gbps, more than sufficient for the packets being transmitted. That capacity is correctly represented in the capacity of the entity queue dedicated to the network.

For the firewalls, the ones chosen are the Palo Alto Serie 3200 and 3400, being the Series 3200 the more restrictive one. They have a throughput capacity that can reach 5 Gbps, again, more than enough for the inputs considered. That capacity is also represented in the queue capacity representing the firewalls. Regarding the processing time of the firewalls, there will be two options. During the first set of simulations, the one closer to reality, the processing time of the firewalls used for this case is variable, it follows two variables, a random value and a value which depends on the size of the packets, following Equation 2:

Equation 2: Firewall's service time in lognormal distribution simulation

$$dt = entity.Mbps \cdot 0.1 + rand(1,1)$$

On the other hand, on the critical conditions simulation the processing time will be considered fast (0.01 seconds), that fastness is also programmed in the server's, used to represent the firewalls, process time.

Moreover, the model used to simulate the failure of any of the firewalls from the network follows the same structure and behaviour as the one used in the active-active configuration from last section. The main difference is that in the current architecture's case, if the SPF fails, all the information that needs to go through the device is blocked until repaired. But, besides that aspect, the coding and conditions remain the same. An example of one of those models proposed is shown in Figure 6.

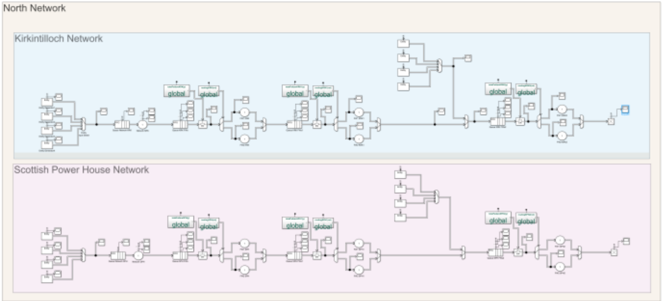


Figure 6: Proposed architecture North Network

B. *Normal conditions analysis*

This subsection will analyse the different performance results coming from the current and proposed architecture models. The probability of failure from the models will follow an Extreme Value Distribution with a sigma of 3. These results will have the results more similar to reality, since the probability of failure is really low. Lastly, the simulation will last 100 seconds.

In normal conditions, there is no failure expected from any of the firewalls since the technologies are recognized to be hugely reliable. The total throughput from both architectures studied change, for this case the new architecture is capable of filtering and transmitting more pockets.

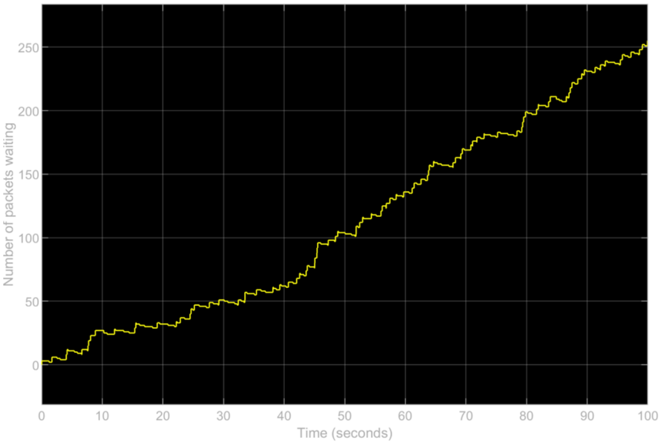


Figure 7: Current architecture, waiting time from one firewall under normal conditions (SPH)

Furthermore, something noticeable is how the limit capacity of the firewalls will be reached slower with the proposed architecture, compared to the current one. This can be clearly seen comparing Figure 7 and Figure 8.

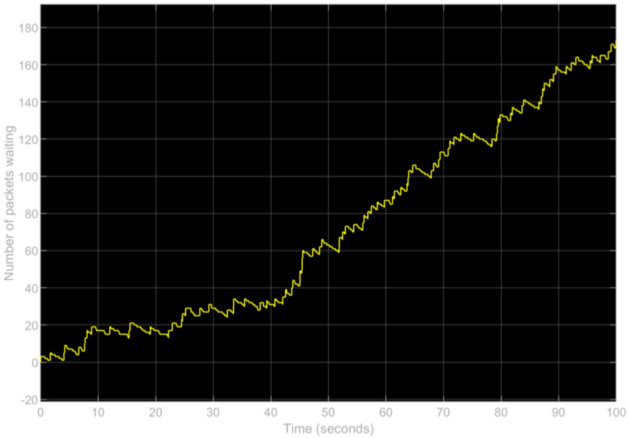


Figure 8: Proposed architecture, waiting time from one firewall under normal conditions (SPH)

C. *Critical conditions analysis*

In critical conditions, failures have occurred in both architectures. The current architecture was incapable of transmitting information from one of the packets generating points (Telecom network), while the proposed one kept transmitting thanks to the availability from the other firewall of the pair. This created a scenario in which, even when the proposed architecture suffered from three times more failure events, the proposed architecture was capable to transmit nearly 50% more packets than the current architecture. Table 3 shows a summarize of the performance results of one the networks (KRK) from both systems.

Table 3: Current and proposed performance results under critical conditions (KRK)

Architecture	Current	Proposed
Total throughput (packets)	416	608
Failure events	1	3

IX. CONCLUSIONS & FUTURE WORKS

This project intention was to analyse the different technologies, techniques and configurations that could be helpful in Scottish Power firewalls architecture to achieve a high redundancy and availability network. To achieve that end goal, a study on the different technologies available in the market was carried, concluding that a complete change to Palo Alto new generation firewalls (NGFWs) was the most beneficial due to, not only the updated capabilities, but also because of the possibility to manage and supervise all assets by one only software, Panorama. Most of the firewalls connected to the architecture will operate in Level 3 of the Purdue Model, the control level, the exceptions will be the firewalls connected to the corporate/enterprise network, which will be in Level 3.5 as DMZ, and the firewalls connected to the devices from Level 2, which will be part of Level 2.5.

Once the technologies for the future architecture were chosen, a first study of the operation of those technologies was done. Their high availability (HA) configurations were analysed, from a technical view, looking into the characteristics of those configurations to look which would be more reliable in the desired future system. That analysis was then followed by a practical analysis, in which simulations were performed and the performance results of the different configurations available on Palo Alto's NGFWs were revised. That technical and practical analysis helped to come with the conclusion that active-active configuration was the one which would provide with most benefits, even if this choice carried an increase in the complexity of the operation of the architecture.

Moreover, a high-level analysis on the routing landscape was performed. The routing techniques used in the different networks from Scottish Power were studied, concluding that North and South use different strategies. The North network relied more in static routing techniques, while the use of dynamic routing techniques was more usual in the South Network. The list of recommendations to update and optimize the current routing landscape are the following: summarization techniques to limit routes and complexity on the routing, the use of router ID and process ID to improve consistency and summarization, the authentication between OSPF neighbours to achieve higher security, and finally, reducing the routing area and the OSPF flood, reducing complexity overall.

Finally, a new architecture consoling the management and supervision of the Infrastructure Firewall Estate, uniting RTS and Telecommunications networks, was proposed. This new architecture was composed in a whole by pair of firewalls from Palo Alto NGFWs, creating HA clusters of firewalls, all operated with the help of Panorama software. Also, the proposed architecture will be symmetric between North and South network, reducing complexity in its operation and management. Once al technical specifications from this proposed architecture were stablished, other simulations were performed to see the behaviour of both, the current and the proposed architecture. Those simulations showed how in normal conditions, were the firewalls have a low probability to fail, the performance of the proposed systems was more beneficial in terms of efficiency and total throughput. The main change from both architectures is that, in normal conditions, in systems with a firewalls cluster where there is only one single firewall, the system will be more congested at that point, which at the end could cause problematics in terms of processing capacity. Moreover, in critical conditions, were failures occurred more often, the proposed architecture showed a great superiority in terms of total throughput performance compared to the current architecture. All those updates showed how there would be an improvement in the performance on the network, which at the end it means that the proposed architecture will be more secure and reliable, and with high availability and redundancy capabilities.

Future works, related to this project could discuss the real problematics that an active-active configuration of the architecture's firewalls could generate. Problems such as asymmetric routing or an undesired and uncontrolled increase in the complexity of the operation and management of the system and its firewalls would need to be covered to have a clear view on how those changes will really affect the architecture at the end.

X. References

[1] Cisco FirePower 2100 Series Data Sheet. https://www.cisco.com/c/en/us/products/collateral/security/firepower-2100-series/datasheet-c78-742473.html

[2] Palo Alto 3200 Series Data Sheet. https://www.paloaltonetworks.co.uk/resources/datasheets/pa-3200-series

[3] Palo Alto 3400 Series Data Sheet. https://www.paloaltonetworks.com/resources/datasheets/pa-3400-series

[4] SimEvents Library – Model and simulate message communication and discrete-event systems. https://uk.mathworks.com/products/simevents.html